

available at www.sciencedirect.comjournal homepage: www.elsevier.com/locate/cose
**Computers
&
Security**


Ethical decision making: Improving the quality of acceptable use policies

A.B. Ruighaver^a, S.B. Maynard^{b,*}, M. Warren^a

^a School of Information Systems, Deakin University, Melbourne, Australia

^b Department of Information Systems, University of Melbourne, Melbourne 3010, Australia

ARTICLE INFO

Article history:

Received 18 August 2009

Received in revised form

7 May 2010

Accepted 11 May 2010

Keywords:

Acceptable use policies

Consequential ethics

Ethical decision making

Security policy quality

Security management

ABSTRACT

While there is extensive literature on the positive effects of institutionalising ethics in organisational culture, our extensive research in information security culture has found no evidence of organisations encouraging ethical decision making in situations where information security might be at risk. Security policies, in particular acceptable use policies, have traditionally been written with a strategy of deterrence in mind, but in practice they rely mostly on deontological ethics, i.e. employees doing the right thing, to work. As far back as 1990, evidence has been reported of a widening socio-technical gap, where employees no longer always act according to expected social norms in an organisation. This change in moral behaviour is reducing the effectiveness of acceptable use policies in an organisation. In this paper, an alternative approach to the development of security policies is proposed to encourage ethical decision making based on consequential ethics. Acceptable use policies will need to distinguish between guidelines, standards and procedures, and guidelines will need to be written in such a way that the policy continuously acknowledges that employees are no longer expected to blindly follow these guidelines. And, as acceptable use policies can no longer cover all the possible risks related to an employee's behaviour, the policy will need to emphasise both explicitly and implicitly that employees are expected to make an ethical judgement on all their actions that may possibly endanger the organisation's security. This will in turn have positive effects on the usability and suitability of the acceptable use policy to the organisation.

Crown Copyright © 2010 Published by Elsevier Ltd. All rights reserved.

1. Introduction

While the literature on information security often indicates the importance of considering ethics in a comprehensive approach to information security (Hartmann, 1995; McDermond, 2008; Sims, 1991), the author's research on security culture and security governance over the past decade (Chia et al., 2003; Ruighaver and Maynard, 2006; Ruighaver et al., 2007) has given no indication that any of the over 20 Australian

organisations involved in our case studies has ever even looked at the ethical aspects of their security approach. This has also been true in research conducted into the quality of security policies at a strategic level within organisations (Maynard and Ruighaver, 2007).

The positive effects of institutionalising ethics upon organisational culture are widely reported (Sims, 1991), but the lack of concrete guidance on how to apply ethics to information security (Von Solms, 2005) is, in our view, one of

* Corresponding author. Tel.: +61 3 8344 1573; fax: +61 3 9349 4596.

E-mail addresses: tobias@deakin.edu.au (A.B. Ruighaver), seanbm@unimelb.edu.au (S.B. Maynard), matthew.warren@deakin.edu.au (M. Warren).

0167-4048/\$ – see front matter Crown Copyright © 2010 Published by Elsevier Ltd. All rights reserved.

doi:10.1016/j.cose.2010.05.004

the main factors that inhibits the practical use of ethics to improve information security in organisations.

This paper aims to explore the practical application of ethics to improve the quality and effectiveness of security policies, in particular that of acceptable use policies. The approach explored in this paper was first proposed by [Ruighaver \(2008\)](#) and originates from that author's initial frustration with a (perceived) lack of ethical behaviour of end-users. This perceived lack of ethics seems to make enforcing the current, traditionally rule based, acceptable use policies a difficult and, more importantly, expensive endeavour. Our current view, however, is that it may not be the end-users ethics that is at fault at all, but rather the manner in which organisations use acceptable use policies to influence user behaviour.

As a result, we believe that the suitability and usability of the traditional acceptable use policy is compromised. For instance, security policy is one of the few remaining areas in organisations where deterrence, rather than positive motivation, is used to coerce people into meeting policy requirements. Altering this perception within policy will improve the suitability of policies to employees and will improve the usability of these policies. Suitability and usability are only two aspects of policy quality ([Maynard and Ruighaver, 2007](#)) that will be improved by the adoption of our approach to support ethical decision making.

In the following section we will discuss why, in our view, the traditional approach to acceptable security policies no longer works. We will follow this with a section on ethics and security policies, where we suggest that the initial perceived lack of ethical behaviour can possibly be explained more positively as a change in how employees make ethical decisions. We will then explore how to develop acceptable use policies to support ethical decision making and the resulting impact of such an approach on the quality of these policies. The final section will discuss an initial case study investigating an attempt to implement a more consequential based approach to acceptable use policy.

2. Traditional security policy development

Traditional acceptable use policies are prescriptive in nature, detailing which behaviour is expected and which behaviour is not allowed. Although the development of these policies is intended to be guided by the risks that need to be controlled ([Lichtenstein, 1997](#)), acceptable use policies rarely link prescribed behaviour to risk, nor do they give any other rationale for why a specific behaviour is good or bad.

Current research on the quality of security policies is limited ([Maynard and Ruighaver, 2003](#)). Our own research on security policy quality has until now been aimed at strategic security policies ([Maynard and Ruighaver, 2006](#)). While this research has resulted in a comprehensive framework for security policy quality, its application to acceptable use policies still needs to be investigated. In practice, the effectiveness of traditional acceptable use policies depends primarily on the quality of the organisation's information security awareness program ([Siponen, 2000](#)) that supports these policies.

As security awareness programs are relatively expensive, many organisations instead rely mainly on deterrence for

their acceptable use policies to work. Each policy outlines what punishments the organisation can use to enforce acceptable behaviour, but again the effectiveness of deterrence depends on what enforcement program is in place to support deterrence. While simply listing the punishments might have worked a decade ago, nowadays deterrence only works if the employees feel that the organisation is serious about enforcing the policy and believe there is a reasonable chance they will be held to account ([Stafford and Warr, 1993](#)).

Deterrence should really only be used for a few high risk behavioural patterns that can be identified without intrusive monitoring. Even then, any practical strategy of deterrence depends on regular monitoring of behavioural patterns to identify when unacceptable behaviour occurs. Unfortunately, monitoring of behaviour and punishment of minor unacceptable behaviour will, in most cases, be detrimental to the general organisational culture. Without monitoring, however, unacceptable behaviour may often become so common that it is no longer possible to make an example of a single employee when that unacceptable behaviour leads to a serious incident. It should also be realised that deterrence is often further undermined by any lack of action when that unacceptable behaviour is first identified. In organisations where employees have been consistently working outside the policy an alternate policy is created – in such a case it is no longer the written policies that are important, instead the different ways of working are considered to mirror the “real” policy.

To reduce the emphasis on deterrence, we propose a new approach to acceptable use policy development based on ethical decision making. While there has been a massive increase in popularity of research aimed at changing an organisation's security culture ([Schlienger and Teufel, 2002](#)) to increase employee adherence to security policies, our research in security culture ([Ruighaver and Maynard, 2006](#)) aims to better align it with organisational culture. As a result, we believe that a better approach is to align the acceptable use policy with the organisational culture. The aim is not to radically change the organisations culture, but to design the acceptable use policy so that it complements the current organisation's culture. So, unless the organisation's culture supports strict adherence to business procedures and standards, their security should not be based on strict adherence to behavioural guidelines. Instead, we propose that the organisation's security policies should support ethical decision making based on the organisation's security objectives.

3. Ethics and security policies

According to [Leiwo and Heikkuri \(1998\)](#), the use of ethics in information systems and information security has two purposes: to identify criteria between good and bad and to promote good desires over bad ones.

In practice, current acceptable use policies rely mostly on deontological ethics, i.e. employees doing the right thing, to work. However, changes in ethical beliefs from the “baby-boomer” generation to “generation-X” and “generation-Y” means that the later generations feel less obliged to adhere to rules. They don't judge the morality of their actions on rules, but rather on the perceived consequences. Current acceptable

use policies still mostly identify good and bad behaviour and rarely identify the criteria that have been used to distinguish “good” from “bad”. Additionally they do not identify the repercussions of engaging in “bad” behaviour for the organisation’s information security, making it difficult to judge the consequences of those actions. These policies also concentrate too much on promoting good behaviour itself, instead of trying to address the underlying reasons why users do behave in a certain way. In particular, current policies do not attempt to influence the user’s beliefs and attitudes that are responsible for creating unacceptable behaviour (Kabay, 1993).

As early as 1990, Kowalski (1990) described how the existence of a socio-technical gap results in a need to address the inconsistency between socially expected norms and computer security policies. Since then, society as well as business ethics has changed significantly, while the prescriptive approach used in acceptable use policies to control the behaviour of IT user’s has hardly changed at all. It is therefore no surprise that the effectiveness of acceptable use policies to prevent computer abuse and other security problems has diminished severely over the past decades (Hone and Eloff, 2002).

Our current approach to address this socio-technical gap in acceptable use policy development is based on the assumption that the behaviour of IT users is no longer primarily based on following rules, but that most users are willing to consider the consequences that their behaviour might have for the organisation. Hence, we suggest that acceptable use policies will need to support decision making based on consequential ethics. In consequential ethics the ethical value of an action is determined by the outcome, even though the action itself may not be ethical.

Of course, it can never be the role of a security policy to teach ethical behaviour. We have to assume that the organisation encourages its employees to behave according to a code of ethics. This can either be a specific code of ethics for that organisation or a more general code of ethics used in industry. Unfortunately, our initial research in organisational ethics indicates that many organisations still use a code of ethics based on an, in our view out of date, deontological ethics approach as well. At the same time, anecdotal evidence also suggests that not all employees are willing to always put the organisation’s best interests above their own self-interest.

If the organisation has not addressed these issues yet, or does not have an ethical code of conduct, it may be worthwhile for its security manager to suggest that providing guidance on ethical behaviour and decision making has positive effects on the organisational culture in general and should therefore not be judged an investment in security alone. Certainly, it would be in the best interest of the organisation to have an ethics program that identifies any employees or groups that do not always have the organisation’s interest at heart and then targets them with a psycho-social education program to change their beliefs and attitudes about ethics.

4. Encouraging ethical decision making

The question we try to address in this section is how to write acceptable use policies in such a way that employees are

encouraged to think about the consequences of their actions and make an ethical judgement. At the same time, we have to acknowledge that not every organisation has institutionalised ethics in their organisational culture, so the approach needs to be useful even when ethical behaviour is not generally encouraged.

While it has become clear that it is no longer sufficient to emphasise deterrence by just listing the punishments the organisation can apply, it may still be useful to ensure that the organisation has some leverage when employees clearly have not considered the consequences of their actions. Organisations should still emphasise that it is unacceptable for employees to endanger the security of the organisation, and organisations should have the option of taking action when employees refuse to behave in an acceptable manner after repeated warnings that the organisation does not agree with their ethical behaviour.

We believe that the first, and probably most important, change in the way we write security policies is to acknowledge that employees are no longer expected to blindly follow all of its advice on acceptable behaviour. Most other policies in organisations only contain guidelines and employees are used to the organisation distinguishing between policies, standards and procedures. A clear distinction between security guidelines, security standards (in the organisation) and security procedures within the acceptable use policy will help employees understand when they are allowed to consider trade-offs between their behaviour and the organisations security objectives and when the organisation expects strict adherence to its norms.

In acknowledging that guidelines are now just that, guidelines, the acceptable use policy will also need to explicitly emphasise that employees are expected to make an ethical judgement and justify their decision when they deviate from these guidelines. If the organisation does not have an ethical code of conduct stating that employees are, in general, expected to follow organisational policies regarding work practices, the policy itself may have to explicitly emphasise that deviating from these guidelines should be an exception (e.g. if you make a habit of not following any guidelines in the policy your conduct is not ethical). It may also be useful to describe the process that employees should follow if they foresee that the same deviation of guidelines will become a regular occurrence or when they believe that the same ethical decision may have to be made by other employees as well. This is similar to what Leiwo and Heikkuri (1998) have called ethics negotiation in their paper on security of distributed systems.

Ethical decision making is not possible if the acceptable use policy does not clearly state its security objectives. Hence, the policy will need to identify the risk for the organisation resulting from an employee’s behaviour, the seriousness of that risk, and how the organisation would like to control that risk. To further support ethical decision making, the policy may also need to identify potential ethical conflicts and other trade-offs that can influence the employees ethical decision making. Another ethical consideration is the language and the country that the policy is developed; Wood (1996) argues that the word “shall” should be avoided in policies, guidelines and standards. This is because (at least in the United States) the word “shall” has a very specific legal meaning.

All of this will clearly increase the size of a policy, but by emphasising the risks over behaviours, there will be no need to cover all possible behaviours. The policy will need to emphasise, both explicitly and implicitly, that employees are expected to always make an ethical judgement of any actions that may possibly endanger the organisation's security. Incorporating these changes will improve the suitability of the acceptable use policy for those employees that belong to those generations that don't automatically follow rules anymore. Suitability is a measure of how appropriate the acceptable use policy is to the organisation (Maynard and Ruighaver, 2007), in particular the extent to which it is aligned with the organisation's culture. Adopting this approach will also improve the usability of the acceptable use policy. As those affected by the policy are made aware of why behaviours are acceptable or unacceptable the effort for employees to utilise and operationalize the policy is likely to be decreased.

In our view the principle aim of the acceptable use policy is to change employee behaviour by making them aware of the objectives of the organisation and the consequences of their actions in relation to these objectives. When an employee does not agree with these objectives, this should not really be considered a security problem. Changing an employee's beliefs and attitudes in relation to the organisation's goals and objectives is rather, an ethics problem that should be addressed by the organisation's ethical standards.

An interesting aspect of the need to discuss potential consequences of a user's behaviour, is the question "*which of the many potential consequences need to be emphasized to best influence their beliefs, attitude and behaviour?*". Our previous experiences in risk management research indicate anecdotally that people have problems relating to low frequency incidents with a high impact and often prefer to concentrate on high frequency incidents with medium impact. A case study, for instance, on an Australian Labour MP, who's son had access to his father's Parliament House work computer (McDermind, 2008), could be an excellent example of what ethical issues arise from allowing other people access to your account. The case study also highlighted the problems that an organisation faces when dealing with a security incident, when the problem is not a technical but a human problem. In terms of this case study, will understanding the ethical concerns influence an employees' ethical decision making, or would a simple statement on the possibility of children accidentally erasing important files have a bigger impact on a user's behaviour?

As discussed before, acceptable use policies, in general, have to rely on expensive support programs to motivate employees to adhere to the policy. In this case the emphasis is on ethics, not security, and if the organisation does not yet have a reward system that rewards ethical behaviour one will need to be set up. Again, the cost of such a system should not be counted towards the security budget. The positive effect of encouraging ethical behaviour will benefit the whole organisation, not just its security.

One major benefit of this ethical decision making approach to acceptable use policies is that the organisation's ethics code is likely to encourage a shared sense of responsibility and accountability. Hence, it is important that the acceptable use policy also emphasises a shared sense of responsibility and

accountability and provides examples on how to cope with the ethical conflicts it produces. While security programs that rely on fellow employees to discourage high risk behaviours and provide feedback on potential security problems are not new, in practice the cost of such programs have limited their use. Again, because the scope of such programs will now target ethical behaviour in general, there will be no need to consider it an investment in security.

From a legal perspective this approach will also bring the security policy style and language into alignment with other policies within the organisation such as various Human Resource policies. Many organisations already use consequential language in their Human Resource policies. As with current acceptable use policies, it is normal for these human resource policies to be vetted by the organisation's legal team. Hence, changing the acceptable use policy ethical approach to a consequential ethics approach should not impact on this procedure.

5. Application of consequential ethics for acceptable use policies

One of the most practical examples of a consequential ethics approach is illustrated by the following case study conducted within a medium sized Australian IT service provider, which we will call *ITOrganisation*. The second author of this study collected the bulk of the data through conducting interviews with multiple stakeholders (12 interviews) across all areas and levels of the organisation in 2005 and 2006. Interviewees were asked a set of guideline questions based on their interaction with and knowledge of the organisation's security policies. Additionally, documentation about the organisation and its security practices was gathered and used to help to triangulate our findings. The researcher had a very hands off role within the organisation and did not influence the development of the policies in any manner.

ITOrganisation is a medium sized, publicly owned organisation based in an Australian Capital City, with offices in 5 countries employing over 250 staff. Their main business is the operation of IT related internet services. *ITOrganisation* has employed security policies within the organisation since early 2000. These policies were initially developed by one of the IT research personnel and were focused purely on telling employees what they were and were not able to do with regards to security. This rule based implementation of the organisations security policies when applied in the organisation were accompanied by a simple statement – "You must abide by this". As a result, as one of the senior managers commented, "*It was very much a document I felt that was put on the shelf and not referenced*" (senior manager 4).

At the time of the case study, the organisation was in the process of redeveloping their whole suite of security policies ranging from the strategic level through to the operational level acceptable use policies. It was clear to the Management of *ITOrganisation* that their current set of policies were quite prescriptive, and within the policies their prescriptions were not backed up with any reasoning or links to the risks identified in the organisation. As such, it was clear that these acceptable use policies were usually put on a shelf and were ill

used by employees, even though an ongoing awareness program was present in the organisation. A result of this was that the policies developed in this manner were deemed a failure with many employees openly admitting they did not comply with the policy as they were unaware of the impact that their non compliance may have on the organisation.

After the failure of the previous policy decision making process, the focus in the organisation was on the implementability of the policy within the organisation, ensuring that it would be used and understood by its employees. During the new policy development process a large amount of discussion took place regarding obtaining the information to create the policy and an understanding was gained for the development team about what would and what would not work from an implementation perspective. *“The redevelopment of security policy was useful. It forces staff to think in security terms, not from a technical basis so much, but from an employee basis. It increases the awareness of employees which is paramount to the organisation”* (senior manager 1). It became clear to the management of ITOrganisation that it was important for employees to understand what it all means if they are to actively implement the policies as part of their day to day work. This resulted in a change in how ITOrganisation regarded security policy and a shift was made changing how the security policies were named, for instance “acceptable use policy” became “acceptable use guidelines”. This reflected the change in the thinking of the organisation and their shift to consequential ethics, over their traditional deontological ethics perspective when dealing with security policy. The organisation’s employees can now be guided towards good ethical behaviour through the acceptable use guidelines and will need to make an ethical judgement and justify it if they deviate from the guidelines.

Consequentially, this brings the security policy in line with other organisational policies where it is made clear to employees that they are responsible for their actions and that these are the consequences of your actions for the organisation if you do not comply with the policy (or guidelines as they were referred to internally). The reasoning behind this focus on policy is best given by one of the senior executives who states *“There are a number, several things. In fact the document is important for people to become aware that the most important thing is the thinking that goes into the document. So for me, being in charge of the risk program it means that we the company has sat down and thought about this, we understand and are aware where our risks lie, it’s not that we shouldn’t take these risks, because if you don’t take risks you won’t make any money, its more about how we think through the risks that we are taking, how we mitigate and control those risks. That shows me that we have done that and if that is practicable then we have actually got something that we can apply in the business and that is effective”* (senior manager 3).

Through changing the “between the lines” meaning of the acceptable use policy, making it a set of acceptable use guidelines for employees, ITOrganisation found that employees were more amenable to following the acceptable use guidelines as they did not tell them what to do, but rather explained the consequences of their actions if they deviated from the guidelines. This had follow on effects within the organisations security awareness program. The program now, rather than simply outlining the policy, was made stronger as they were

able to clearly identify the risks addressed by the policy and directly show the consequences of not following the acceptable use guidelines on the organisation’s security. Not emphasising the consequences for the employees (punishment), but addressing motivation instead, did in turn improve the culture of the organisation when dealing with its security as a whole. Now, employees had the responsibility and accountability of their actions towards the acceptable use guidelines. One of the best outcomes was summarised by a lower level employee in the organisation who states that whilst the guidelines impact the ways in which they work, that they also make them think about the consequences of giving out information they are asked for by their customers. *“it’s a good thing... I’m quite confident and I feel quite comfortable in telling a customer that I cannot give you something, rather than not following the guidelines and giving them something I shouldn’t”* (lower level employee 3).

6. Conclusion

To combat the diminishing effectiveness of traditional acceptable use policies, we have proposed a new approach based on the assumption that ethical behaviour of employees nowadays is mainly based on consequential ethics. We believe that employees are, in general, no longer accepting the organisation’s suggestions on what is good or bad behaviour, but may be willing to consider the consequences of their actions for the security of the organisation.

Implementing support for decision making based on consequential ethics in acceptable use policies does not require much more than just some common sense. Making a distinction in the policy between guidelines and standards is an obvious step to ensure employees know when they are allowed to make decisions based on consequential ethics and when the organisation will not accept any deviation of behaviour.

As consequential ethics is based on the consequences of actions for both the employee and the organisation it should also be obvious that, to support ethical decision making, the policy will need to provide the insights on why, and under what circumstances, certain behaviours are acceptable or unacceptable. The advantage is that employees will now become aware of the consequences many of their actions will have for the security of the organisation, which will assist them in unforeseen situations.

Finally, the surprising side effect of this approach to promote acceptable user behaviour is that much of the expensive “awareness programs” will now no longer just be about information security. If the organisation already has programs to support ethical behaviour, they can simply incorporate the necessary examples related to information security. This, subsequently, should negate the need to have separate reward systems to motivate employees about information security.

We are currently looking for an organisation willing to participate and fund longitudinal action research to investigate the most effective way to implement a consequential ethics approach to acceptable use policies.

REFERENCES

- Chia P, Maynard S, Ruighaver AB. Understanding organisational security culture. In: Hunter MG, Dhanda KK, editors. *Information systems: the challenges of theory and practice*. Las Vegas, USA: Information Institute; 2003. p. 335–65.
- Hartmann A. Comprehensive information technology security: a new approach to respond ethical and social issues surrounding information security in the 21st century. In: IFIP TC11 11th international conference of information systems security, 1995.
- Hone K, Eloff JHP. What makes an effective information security policy? *Network Security* 2002;2002(6):14–6.
- Kabay ME. Social psychology and infosec: psycho-social factors in the implementation of information security policy. In: *Proceedings of the 16th national computer security conference*, Baltimore, MD, USA, September 20–23, 1993.
- Kowalski S. Computer ethics and computer abuse: a longitudinal study of Swedish university students. In: IFIP TC11 6th international conference on information systems security, 1990.
- Leiwo J, Heikkuri S. An analysis of ethics as foundation of information security in distributed systems. In: *Proceedings of the thirty-first annual Hawaii international conference on system sciences*. vol. 6; 1998. p. 213.
- Lichtenstein S. Developing internet security policy for organisations. In: *Proceedings of the 30th Hawaii international conference on system sciences: information systems track – internet and the digital economy*, January 03–06, 1997. p. 350.
- Maynard S, Ruighaver AB. Development and evaluation of information system security policies. In: Hunter MG, Dhanda KK, editors. *Information systems: the challenges of theory and practice*. Las Vegas, USA: Information Institute; 2003. p. 366–93.
- Maynard S, Ruighaver AB. What makes a good information security policy: a preliminary framework for evaluating security policy quality. In: *5th annual security conference*, Las Vegas, Nevada USA, 19–20 April, 2006.
- Maynard SB, Ruighaver AB. Security policy quality: a multiple constituency perspective. In: Dhillon G, editor. *Assuring business processes*, proc. of the 6th annual security conference. Washington DC: Global Publishing, USA; 11–12 April 2007.
- McDermind D. *Ethics in ICT: an Australian perspective*. Pearson Education Australia; ISBN 9780733993879; 2008.
- Ruighaver AB, Maynard S. Organisational security culture: more than just an end-user phenomenon. In: *Proceedings of the 21st IFIP TC-11 International Information Security Conference (IFIP/SEC 2006)*, May 22, 2006, Karlstad, Sweden; 2006. p. 425–430.
- Ruighaver AB, Maynard S, Chang S. Organisational security culture: extending the end-user perspective. *Computers & Security* February 2007;26(1):56–62.
- Ruighaver AB. Encouraging ethical decision making in security policies. In: *Fifth Australian institute of computer ethics conference AiCE 2008*, Melbourne, February 11 2008.
- Schlienger T, Teufel S. Information security culture – the socio-cultural dimension in information security management. In: *IFIP TC11 international conference on information security*, Cairo, Egypt, 2002.
- Sims RR. The institutionalization of organisational ethics. *Journal of Business Ethics* 1991;10(7).
- Siponen MT. On the role of human morality in information system security: the problems of descriptivism and non-descriptive foundations. In: *Proceedings of the IFIP TC11 fifteenth annual working conference on information security for global information infrastructures*, 2000. p. 401–410.
- Stafford M, Warr M. A reconceptualization of general and specific deterrence. *Journal of Research in Crime and Delinquency* 1993;30:123–35.
- Von Solms E. *Institutionalizing information security*, Msc. thesis, University of Johannesburg, South Africa; 2005.
- Wood CC. *Information security policies made easy* (version 5); 1996. Baseline Software.
- Sean Maynard** is a lecturer in the Department of Information Systems at the University of Melbourne. Starting his academic career in Information Systems focusing on the use of computing technology to aid senior management (EIS) and the evaluation of decision support systems, his research over the past decade has been in the area of information systems security, in particular focusing on the evaluation of security policy quality and on the investigation of security culture within organisations. Sean also has interests in logistics and supply chain management with a focus on the simulation of the logistics supply chain.
- Dr. A.B. (Tobias) Ruighaver** is a retired academic, who continues his research in information security and computer forensics as an Honorary Fellow at both Deakin University and the University of Melbourne in Australia. He still supervises several Ph.D. students and maintains a website on security governance and security culture at www.securitygovernance.net. Before his retirement Dr. Ruighaver was the head of the Organisational Information Security Group at the University of Melbourne and supervised in depth case study research in over 30 Australian and Singaporean organisations to investigate their security culture, security governance and/or risk assessment practices.
- Professor Warren** has published in the areas of Information Security, Risk Analysis, eBusiness, Information Warfare and Critical Infrastructure Protection. He has authored/co-authored over 225 books, book chapters, journal papers and conference papers. Professor Warren is the former Chair of IFIP TC 11 Working Group 11.1 Security Management and a former Director of the Australian Institute of Computer Ethics. Professor Warren has taught within Australia, Finland, Hong Kong and the UK.